A screenshot of a cell phone

Description automatically generated

**Addendum REST Document**

SSO Documentation Addendum

### The Standard: Regular SSO to MRP using SOAP & REST API

**IMPORTANT!: JWT Storage Path will not be supported any further. Only Use Regaular SSO SOAP and REST API combo path. Further details below about this path.**

#### **Regular SSO addendum : Previous documentation is still valid, this is offered as a more detailed explanation.**

**Regular SSO: The SETUP**

1. **Authenticate user credentials via existing platform.**
2. **Generate SOAP SSO token using already built functionality (SOAP API Token Generation)**
3. **Instead of posting token to P4 login page**
   1. **i) Post SSO token to regularSSO endpoint (platform/v1/regularSSO)**
   2. **ii) Payload format is ‘token=[TOKEN.VALUE]&nextURL=[NEXTURL.VALUE]&logoutURL=[LOGOUTURL.VALUE]’**

**iii) There are also URLs in MRP Configs that need to be populated for the full functioning of SSO.**

**Go to Console -> Association -> Setup -> MRP Settings -> SSO Configs**

1. **If token is valid the REST API will generate a url in the format of**

***https://xxxx.users.membersuite.com/auth/sso?tokenGUID=c71ab416-738e-480d-a6f2-1fafb93654ed&nextUrl=&returnText=&logoutUrl=***

1. **The nextUrl will pass the url in a base 64 encoding to preserve referential integrity to the next url.**
2. **If you need to create a session redirect to this URL and an MRP session will be created with that user signed onto MRP.**

**Regular SSO (continued)**

#### **Regular SSO addendum : Previous documentation is still valid, this is offered as a more detailed explanation.**

**Regular SSO: The ACTION**

**1) Once users are added to the user pool for their particular association, they are set in what AWS Cognito calls a RESET\_REQUIRED status.**

**CASE 1: Users will receive an error when trying to log in due to RESET REQUIRED status in user pool.**

**Options:**

1. **Detect the error coming from the SDK and redirect to the Reset Password page for the association. Reach out via email for the specific URL link.**
2. **Use the SOAP API and offer them a way to RESET their password via SOAP.**

***COMING SOON: we will be pushing out a more customizable page for resetting passwords via the MRP portal. Look for these updates coming soon to all SSO integrators.***

### Reverse SSO

**Reverse SSO modifications**

#### **Reverse SSO addendum**

**Reverse SSO (Start on MS, Go To Third Party Site)**

**1) User is sent from MS to website with 'TokenGUID' query string parameter**

**2) Third Party hits REST API endpoint "GET regularSSO" with TokenGUID and PartitionKey as query string parameters (**[**https://rest.membersuite.com/platform/swagger/ui/index#!/AuthToken/AuthToken\_Get**](https://rest.membersuite.com/platform/swagger/ui/index#!/AuthToken/AuthToken_Get)**)**

**2a) Valid TokenGUID will return Token String value**

1. **Third Party uses Token String value as Authorization Header when hitting REST API endpoint "GET whoAmI" (**[**https://rest.membersuite.com/platform/swagger/ui/index#!/WhoAmI/WhoAmI\_Get**](https://rest.membersuite.com/platform/swagger/ui/index#!/WhoAmI/WhoAmI_Get)

**3a) Valid GET call will return information about the Portal User that generated the original Token String**

**3b) Token String should use "AuthToken" schema, which should be included when using the swagger (i.e. Authorization : AuthToken SyDFOuX+t35sksGHnswBHbB...)**

1. **Third Party uses info returned from "GET whoAmI" (Individual GUID) to create SOAP API search in order to return the required criteria for Third Party access privileges**

**4a) Searches can be built using our SOAP API SDKs, .NET and PHP supported (**[**https://github.com/membersuite**](https://github.com/membersuite)**)**

**4b) AssociationID, PartitionKey, AccessKeyID, & SecretAccessKey are the pieces needed for this implementation. If Third Party needs to generate Tokens (for SSO functionality into MemberSuite), the SigningCertificateID and SigningCertificate.XML file is also required.**